MICRO-CHIPPING AWAY AT PRIVACY: PRIVACY IMPLICATIONS CREATED BY THE NEW QUEENSLAND DRIVER LICENCE PROPOSAL

I INTRODUCTION

Queensland Transport plans to launch its 'New Queensland Driver Licence' Smartcard in 2008.[1] The introduction will commence in November 2008 as a pilot with a complete rollout in July 2009.[2] Delivery of the smartcard driver licence could be through a public-private partnership, with revenue earned through the partnership helping to offset the costs of the new driver licence. [3] The most recent media statement on the proposal, dated January 18 2007, confirmed that shortlisted bidders had been invited to submit binding bids for the development of the new licence.[4] This will make Queensland the first State in Australia to introduce a smartcard driver licence.

Whilst Queensland Transport has specifically addressed issues of privacy in its *Privacy Management Strategy*[5], the use of the smartcard technology will occur despite the absence of clear legislative protections including legal redress for information privacy. The Australian Law Reform Commission (ALRC) in its recent *Review of Australian Privacy Law Discussion Paper (*ALRC *Discussion Paper*) has identified the use of smartcards as raising significant privacy concerns including their lack of anonymity; their ability to collect vast amounts of information; and the ability to generate profiles.[6] It is disappointing that Queensland has failed to implement the recommendations of the 1998 Queensland Legal, Constitutional and Administrative

[1] Premier & Treasurer The Honourable Peter Beattie, 'Smart Licence on the Cards' (Ministerial Media Statement, Thursday, December 29, 2005).
[2] Queensland Transport, *Invitation for Expression of Interest: New Queensland Driver Licence*, Issued 16 August 2006, EOI No. ISB086/06, Department of Public Works Queensland Government Marketplace website, <http://www.projectservices/qld.gov.au/eternderqgm/Tender.asp?TenderID=4764> at 10 September 2006. The EOI was removed on 2 October 2006.
[3] Queensland Transport, *New Queensland Driver Licence Proposal: Consultation Paper*, September 2003, 5.
[4] Queensland Government, Ministerial Media Statement, Minister for Transport & Main Roads, The Honourable Paul Lucas, Thursday, January 18 2007, '*Government shortlists consortia for smartcard driver licence*', <http://statements.cabinet.qld.gov.au/MMS/StatementDisplaySingle.aspx?id=49949> at 10 January 2008.
[5] Queensland Transport, *New Queensland Driver Licence: Privacy Management Strategy* (2003)
[6] Australian Law Reform Commission, *Review of Australian Privacy Law*, Discussion Paper 72,(2007) 328–329.

Review Committee's Report on *Privacy in Queensland*[7] that would have created adequate protections for privacy as a means of balancing the privacy concerns associated with smartcards. This article considers the privacy implications associated with the NQDL Proposal particularly in the absence of state privacy legislation. It concludes that information privacy legislation in Queensland is required as a matter of priority.

II OVERVIEW OF THE PROPOSED 'NEW QUEENSLAND DRIVER LICENCE' PROPOSAL

The New Queensland Driver Licence Proposal (NQDL Proposal) includes the smartcard that will be issued to licence-holders and the database that will support the smartcard. The face of the NQDL Smartcard will contain the same information that currently appears on the driver licence. A digital photograph will replace the current wet film photograph; applicants for the driver licence will also provide a digitised signature[8]. The microchip of the driver licence will contain similar information that appears on the face of the driver licence. A number of optional features are also proposed including the ability to store emergency contact details on the microchip; the capacity to perform secure online transactions; and access to commercial services such as loyalty schemes and an e-purse. These services would be 'partitioned' separately from the Queensland Transport driver licensing functions.[9]

Behind the smartcard technology of the driver licence itself, sits the Transport Registration and Integrated Licensing System Database, known as 'TRAILS'. The power to establish the TRAILS database is provided under the *Transport Operations (Road Use Management) Act 1995* (Qld). Personal information stored on TRAILS will include the digital photograph and the digitised signature, and the licensing information. This information will be encrypted. [10] The database will not include the

[7] Queensland Legal, Constitutional and Administrative Review Committee, *Privacy in Queensland*, Report no 9 (1998)
[8] The consultation material on the NQDL refers to a 'digital signature', that is the use of public key technology that applies an algorithm to encrypt a message. However, the NQDL will use a 'digitised signature' – a signature that has been scanned into a computer.
[9] Queensland Transport, *New Queensland Driver Licence Proposal: Consultation Paper* (2003) 3-5.
[10] Queensland Transport, *New Queensland Driver Licence: Privacy Management Strategy* (2003) 3.

emergency contact details.[11] The *NQDL: Consultation Paper* does not specify if the licence holder's traffic offence history would be stored on *TRAILS* or on the microchip.

III OVERVIEW OF SMARTCARD TECHNOLOGY

Smartcard driver licences have been introduced in Argentina, China, El Salvador, Ghana, Guatemala, India, Malaysia and Mexico.[12] In Australia, no other state or territory has (as yet) introduced smartcard technology to administer a driver licence; however it is likely that if Queensland is successful in its implementation of smartcard technology, then other states and territories will follow suit. This conclusion may be supported by Austroad's[13] preparation of a discussion paper in which it provided an interoperability protocol[14] in which the development of 'a national approach to the deployment of smartcard-based driver licences in Australia' is discussed. Queensland and other states already participate in an arrangement enabling the exchange of driver licensing and registration details under the National Exchange of Vehicle and Driver Information System (NEVDIS), authorised in Queensland by the *Transport Operations (Road Use Management – Vehicle Registration) Regulation 1999.*[15]

Smartcards have a number of features that make them useful as a means of data transmission and data storage. Firstly, smartcards contain an embedded microchip that can transmit data either through direct contact with a smartcard reader, in which case the smartcard is known as a contact card, or by being activated through the use of high frequency radio waves that can be transmitted from the card to a transmitter within range. This latter type of card, known as contactless, has been used mostly for

[11] Ibid 8.
[12] VicRoads, *Introducing New Driver Licence Card Technologies: A Smarter Licence for Victorians* (2002) 9.
[13] Austroads is the association of Australian and New Zealand Governments road transport and traffic authorities. Austroads members are the six Australian state and two territory road transport and traffic authorities, the Commonwealth Department of Transport and Regional Services, the Australian Local Government Association and Transit New Zealand.
[14] Austroads, *Smartcard Licence Interoperability Protocol (SLIP): A flexible approach to driver licensing into the future,* Discussion Paper (2005) 3.
[15] *Transport Operations (Road Use Management – Vehicle Registration) Regulation 1999* (Qld),Division 5.

high speed or large volume applications, for example, tollways. The NQDL Smartcard will be a contact smartcard.[16]

The second feature of a smartcard that makes it useful is that the smartcard chip may be comprised of partitioned data storage areas or memory facilities. Each of the components can be accessed by different parties involved in the use of the smartcard. This allows the smartcard to be used as a platform to support a number of commercial and government functions. 'Both types of smartcards offer true multi-functionality. The storage and processing capacities of smartcards are impressive, and it is not unusual to find a smartcard that is capable of performing up to fifty different functions.'[17]

With respect to the NQDL Smartcard, information is partitioned to provide for an 'open' part of the chip which contains details of the card holder (name and address); this can be read by anyone with access to a suitable card reader, although the information cannot be overwritten. The 'working' component of the chip contains information that is specifically about the card holder such as the person's driver licensing information. The 'secret' part of the chip contains information that cannot be accessed by the card holder without the use of a personal identification number or password. The 'super secret' part of the chip contains information and programs placed there by the chip manufacturer and/or the issuer of the card. This area can only be accessed by the chip manufacturer.[18]

Queensland Transport foreshadowed using smartcards for driver licences in its submission to the Legal, Constitutional and Administrative Review Committee Report on *Privacy in Queensland*. In its submission, dated 28 July 1997, Queensland Transport stated that 'the possibilities for smartcards are enormous; for example, Queensland Transport is evaluating the possibility of using smartcards as a future replacement for drivers licences in Queensland.'[19]

---

[16] Queensland Transport, *New Queensland Driver Licence Proposal: Consultation Paper* (2003) 9.
[17] Privacy Committee of New South Wales, *Smart Cards: Brother's Little Helpers*, Report, No 66 (1995) 7.
[18] Federal Privacy Commissioner, *Smart cards: Implications for privacy*, Information Paper No 4 (1995) 7.
[19] Queensland Legal, Constitutional and Administrative Review Committee, *Privacy in Queensland*, Report No 9 (1998) 193.

There are also disadvantages associated with smartcard technology that have not been addressed within the policy documents used to advance the NQDL Proposal. The Australian Government *Smartcard Framework, Smartcard Handbook*[20] has identified major security vulnerabilities including direct probing by scanning an electron microscope over the smartcard to reveal its memory contents; 'side channel' attacks, which have been the subject of much academic and private sector research; crypto analysis; and quantum computing. A Sydney University engineering student has '…demonstrated a smartcard attack for his final year thesis, using a method called 'differential power analyses'. Using software he developed and a cathode ray oscilloscope [the student] showed that cards using Data Encryption Standard…. could be interrogated to reveal secret information such as keys and [personal identification number]'.[21]

One of the key objectives put forward by Queensland Transport for using smartcard technology in the NQDL Proposal is its ability to reduce the issue of fraudulent driver licences.[22] This objective might not so easily be achieved given the demonstrations of vulnerabilities associated with the technology. Of Queensland Transport plans to launch its 'New Queensland Driver Licence' Smartcard in 2008. The introduction will commence in November 2008 as a pilot with a complete rollout in July 2009. Delivery of the smartcard driver licence could be through a public-private partnership, with revenue earned through the partnership helping to offset the costs of the new driver licence. The most recent media statement on the proposal, dated January 18 2007, confirmed that shortlisted bidders had been invited to submit binding bids for the development of the new licence. This will make Queensland the first State in Australia to introduce a smartcard driver licence.

Whilst Queensland Transport has specifically addressed issues of privacy in its *Privacy Management Strategy*, the use of the smartcard technology will occur despite the absence of clear legislative protections including legal redress for information privacy. The Australian Law Reform Commission (ALRC) in its recent *Review of*

[20] Australian Government Information Management Office, *Smartcard Handbook* (2006) B2.
[21] Electronic Frontiers Australia, *Queensland Smart Card Driver Licence Proposal* (2003) 4.
[22] Queensland Transport, *New Queensland Driver Licence Proposal: Consultation Paper* (2003) 9-10.

*Australian Privacy Law Discussion Paper (*ALRC *Discussion Paper*) has identified the use of smartcards as raising significant privacy concerns including their lack of anonymity; their ability to collect vast amounts of information; and the ability to generate profiles. It is disappointing that Queensland has failed to implement the recommendations of the 1998 Queensland Legal, Constitutional and Administrative Review Committee's Report on *Privacy in Queensland* that would have created adequate protections for privacy as a means of balancing the privacy concerns associated with smartcards. This article considers the privacy implications associated with the NQDL Proposal particularly in the absence of state privacy legislation. It concludes that information privacy legislation in Queensland is required as a matter of priority. Of course, the counter-argument is that, to date, no technology is absolutely impenetrable.

IV INTEROPERABILITY OF SMARTCARDS

The concept of 'interoperability' is a key feature of smartcards. Already the Australian Government, in its *Smartcard Framework, Responsive Government: A New Service Agenda,*[23] has anticipated the Queensland Government's proposed NQDL Proposal in which all licensed road users' information (personal information, road traffic information, criminal records) will be linked into the Australian Government's *Smartcard Framework.* The Australian Government is anticipating the development of a coordinated network of smartcards potentially through all levels of government (local, state and federal) and out into commercial organisations. The *Smartcard Framework* is intended 'to facilitate clear thinking about implementation issues… to help agencies understand the business case for smartcards, and to promote standardisation and uniformity for the shared benefit of all government agencies.'[24] 'Shared benefit' has the potential to lead to 'function creep' through breaches of, or exceptions to, the information privacy principles that protect collection, use and disclosure of personal information.

[23] Australian Government Information Management Office, *Australian Government Smartcard Framework: Responsive Government – A New Service Agenda* Part A (2006) 8. The set of documents is established by the Australian Government Information Management Office June 2006 (the '*Smartcard Framework* '). The *Smartcard Framework* is intended 'to facilitate clear thinking about implementation issues… to help agencies understand the business case for smartcards, and to promote standardisation and uniformity for the shared benefit of all government agencies.'

[24] Ibid 8.

V OVERVIEW OF INFORMATION PRIVACY REGULATION

The regulation of information privacy in Australia is regulated under a number of regimes including the Commonwealth *Privacy Act 1988 (Cth*) which has application for Commonwealth agencies and the private sector. Information privacy in Queensland is regulated by *Information Standard 42: Information Privacy and Guidelines*, (IS42) an administrative decision of the Queensland Cabinet (made on 13 September 2001) and applying to Queensland State agencies.[25] It applies neither to the private sector, nor to local government.[26]

The ALRC *Discussion Paper* has commented that 'Australian privacy laws are multi-layered, fragmented and inconsistent.'[27] The Senate Legal and Constitutional Reference Committee inquiry, The *Real Big Brother: Inquiry into the Privacy Act 1988* (2005) noted that '[t]his inconsistency occurs across Commonwealth legislation, between Commonwealth and state and territory legislation, and between the public and private sectors.'[28] For example, the *Privacy Act* does not apply to states or territories, yet it does apply to state instrumentalities (state business enterprises).[29]

There is further inconsistency in the comparison of regulation of privacy between Queensland, and other states and territories. Some other jurisdictions throughout Australia[30] have introduced legislation to protect information privacy, including New

---

[25] Queensland Government Information Architecture, *Information Standard 4: Information Privacy Guidelines* (2001).
[26] Health information is regulated by *Information Standard 42A.*
[27] Australian Law Reform Commission, *Review of Australian Privacy Law*, Discussion Paper 72 (2007) 236.
[28] Australian Law Reform Commission, *Review of Australian Privacy Law*, Discussion Paper 72 (2007), 236 quoting the Parliament of Australia - Senate Legal & Constitutional Reference Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005) [7.6].
[29] *Privacy Act 1988* (Cth) ss 6C(4) & 6F. The Office of the Federal Privacy Commissioner provides further information on the complexities of the obligations upon Commonwealth contractors in its *Information Sheet 14 – 2001: Privacy Obligations for Commonwealth Contractors*, Federal Privacy Commissioner's website, < http://www.privacy.gov.au/publications/IS14_01_print.html>, at 14 January 2008.
[30] New South Wales has the *Privacy and Personal Information Protection Act 1998* (NSW) which makes provisions for Information Privacy Principles (Part 2); Privacy codes of practices and management plans (Part 3); Privacy Commissioner (Part 4); and a Privacy Advisory Committee (Part 7). Victoria has the *Information Privacy Act 2000* (Vic) which makes provision for: Information Privacy Principles (Part 3); Codes of practice (Part 4); and a Privacy Commissioner (Part 7). The

South Wales, Victoria, the Australian Capital Territory, the Northern Territory, and Tasmania. Western Australia has prepared an *Information Privacy Bill 2007*, which to date has not yet been passed. South Australia, the only other state reliant upon an administrative approach, at least provides support for the administrative regime with a Privacy Committee proclaimed in 2001.[31]

VI *PRIVACY ACT 1988* (CTH)

The *Privacy Act 1988* (Cth) was passed 'to make provision to protect the privacy of individual, and for related purposes'. The *Privacy Act*, however, protects only 'information privacy'. The *Privacy Act* seeks to achieve this for the Commonwealth public sector through the establishment of eleven Information Privacy Principles[32]. The Information Privacy Principles ('IPPs') relate to collection and use of data (IPPs 1, 2, 3, 9, 10 and 11); storage and security of data (IPPs 4, 5 and 6); and accuracy of data (IPPs 7 and 8). The principles apply to 'personal information' in a 'record'.

'Personal information' is defined[33] as 'information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.' 'Sensitive information' means information or an opinion about an individual's racial or ethnic origin; political opinions or associations; religious or philosophical beliefs; membership of a trade union; sexual preferences; or criminal record. It also includes health and genetic information about an individual.[34] 'Record' means a document, database (however kept) or a photograph or other pictorial representation of a person'.[35]

Australian Capital Territory has the *Information Privacy Act 2000* (ACT) and the Northern Territory has the *Information Act 2004* (NT). Tasmania has the *Personal Information Protection Act 2004* (Tas).

[31] Cabinet Administrative Instruction 1/89 dealing with information privacy. The Privacy Committee was proclaimed in 2001.

[32] *Privacy Act 1988* (Cth) s14.

[33] *Privacy Act 1988* (Cth) s6.

[34] *Privacy Act 1988* (Cth) s6.

[35] *Privacy Act 1988* (Cth) s6.

The TRAILS database and the digital photograph of the NQDL-holder on the NQDL Smartcard could be within the definitions of 'personal information' and possibly 'sensitive information' (that is if the definitions in the *Privacy Act* apply to Queensland agencies under IS42, which is discussed below).

The Biometrics Institute (as cited in the ALRC's *Discussion Paper*) states in its Code that 'a photograph could be described as one of the lower levels of biometric recognition'.[36] The ALRC *Discussion Paper* stated that 'sensitive information should be amended to include certain biometric information… It is very personal because it is information about an individual's physical self. [And] can reveal other sensitive information, such as health or genetic information and racial or ethnic origin. [It] can provide the basis for unjustified discrimination.'[37] The privacy implications associated with the NQDL Smartcard digital photograph, and the sensitive information it can reveal becomes more significant in relation to access to the photograph by Queensland Police Service (see the discussion below).

VII *INFORMATION STANDARD 42 – INFORMATION PRIVACY*

The regulation of privacy for government agencies in Queensland (with the exception of health information) is through Queensland *Information Standard 42: Information Privacy and Guidelines* (IS42).[38] The principles identified in IS42 are based on the 11 IPPs in the *Privacy Act*. It is unclear as to whether or not the definitions of the *Privacy Act* have been imported into IS42. For example, the information standard provides similar definitions to the *Privacy Act* for 'personal information' and for an 'individual', however there is no definition of 'sensitive information', merely the inclusion of the statement that '[c]ollecting personal information will be intrusive if it involves: asking questions about sensitive personal affairs; for example, a person's medical history, their sexual preferences, their personal finances, their political persuasion…'[39]

[36] Australian Law Reform Commission, *Review of Australian Privacy Law*, Discussion Paper 72 (2007), 211 quoting *Biometrics Institute, Biometrics Institute Privacy Code Information Memorandum* (2006), 1.
[37] Ibid 213-214.
[38] Queensland Government Information Architecture, *Information Standard 4: Information Privacy Guidelines* (2001).
[39] Ibid 29.

The standard is administrative with limited enforcement available through a series of codes of conduct, privacy plans and disciplinary actions offered through the *Public Sector Ethics Act 1994*, the *Public Service Act 1996* and the *Financial Administration and Audit Act 1977*.

The information privacy regime available in Queensland is disappointing given the comprehensive review of privacy undertaken by the Queensland Legal, Constitutional and Administrative Review Committee in 1998, in which that Committee gave serious consideration to matters such as: What is privacy, why should it be protected, how is privacy is currently protected in Queensland in terms of information privacy in the public sector and in the private sector.

In its conclusion, the Legal Constitutional and Administrative Committee made 32 recommendations[40], including: That a Queensland Privacy Commissioner or Committee be established by legislation, the *Privacy Act (Qld*)[41]; that the Information Privacy Principles applicable to Queensland government departments and agencies be implemented in legislation and not by cabinet administrative instructions;[42] that the functions of the Queensland Privacy Commissioner should not be combined with any other office;[43] that the *Privacy Act (Qld)* should apply to private service-providers contracted by Queensland government departments and agencies to perform services which would otherwise be performed by those departments or agencies;[44] that a number of privacy issues arise from the use of smartcards and that the Queensland Privacy Commissioner conduct an audit to establish the use or intended use of smartcards.[45]

To date, none of these recommendations made by the Queensland Legal, Constitutional and Administrative Review Committee have been implemented. Indeed in many instances successive Queensland governments have implemented a

[40] Queensland Legal, Constitutional and Administrative Review Committee, *Privacy in Queensland*, Report no 9 (1998) XII–XXI.
[41] Ibid 48. In 1999 an *Information Privacy Bill* was introduced into Queensland Parliament, but not passed.
[42] Ibid 59.
[43] Ibid 119.
[44] Ibid 132.
[45] Ibid 198.

privacy regime that directly conflicts with the recommendations. For example information privacy principles have been implemented by cabinet administrative instructions rather than through legislation; the proposed NQDL Proposal will utilise the already over extended Ombudsman's Office[46] as a means of providing external privacy oversight; Queensland Transport has undertaken an audit of its datasets as part of its *Privacy Plan*,[47] however this remains incomplete in significant areas,[48]; and a smartcard specific audit has not been conducted by government departments.

VIII APPLICATION OF *INFORMATION STANDARD 42* TO THE NQDL PROPOSAL

The analysis of the proposed NQDL Proposal in this article is dealt with in terms of asking 'is the NQDL compliant with the Information Privacy Principles (IPPs) in IS 42?' In particular, compliance is considered in terms of the collection, use and disclosure of personal information.

IX COLLECTION OF INFORMATION

IPP 1 requires that personal information shall not be collected unless it is for a lawful purpose directly related to a function or activity; also, the collection must not be by unlawful or unfair means. The ALRC *Discussion Paper* has stated that 'the Privacy Commissioner has expressed the view that 'purpose of collection' is to be interpreted narrowly, and that agencies should have a clear purpose for collecting each piece of personal information. It is not generally acceptable for an agency to collect information just because it may be useful in the future.'[49]

---

[46] Queensland Transport, *New Queensland Driver Licence: Privacy Management Strategy*,(2003) 13. 'The Ombudsman under the *Ombudsman Act 2001 (Qld)* has broad powers of investigation and these powers would extend to investigations of matters relating to Queensland Transport's data management practices.

[47] Queensland Transport, *Privacy Plan – Information Privacy* (2006) Appendix B.

[48] The incompleteness of the Queensland Transport dataset audit (in the *Queensland Transport Privacy Plan: Information Privacy*, December 2004) was revealed through a cross-referenced check with the Queensland Police Service dataset audit (in the *Queensland Police Service Information Privacy Plan*, 20 July 2004.

[49] Australian Law Reform Commission, *Review of Australian Privacy Law*, Discussion Paper 72 (2007) 600 referring to the Office of the Federal Privacy Commissioner, *Plain English Guidelines to Information Privacy Principle*, 1–3: Advice to Agencies about Collecting Personal Information (1994).

Queensland Transport currently has the legislative authority to collect information for the purposes of maintaining a licensing database under the *Transport Operations (Road Use Management) Act 1995(Qld).*[50] Queensland Transport is proposing an additional 'purpose' provision to be included under this Act, 'that would include a clear definition of the circumstances for collecting driver licensing information.'[51] The inclusion of a 'purpose' provision; the details of its breadth; and any offences attaching will be a critical element in ensuring the protection of personal information. The provision would provide a legislative basis to enable an aggrieved NQDL-holder to challenge such collection of personal information as being *ultra vires* and beyond the statutory purposes under administrative law. To date, however, Queensland Transport has not provided a draft of the 'purpose' provision, nor any outline as to its possible content for public comment.

X USE & DISCLOSURE OF INFORMATION ON THE NQDL

IPP 10 provides for limits on the use of personal information; and IPP 11 provides for limits on the disclosure of personal information. Both IPPs provide for circumstances in which use and disclosure may occur, including that the individual was reasonably likely to have been aware the information would be so disclosed; the individual consented; it was authorised by law; or it was reasonably necessary for enforcement of the criminal law.

The NQDL Proposal provides for a number of uses and disclosures of personal information including to: Queensland Transport licensing staff and authorised officers; interstate licensing authorities; and the Queensland Police Service. Disclosure to Emergency Service officers is on a voluntary basis and so would be within the consent and/or 'reasonably aware' exceptions. Disclosure to commercial operators involves an analysis of the contracts under the public-private partnership in

[50] *Transport Operations (Road Use Management) Act 1995* (Qld) s 3(a) provides that 'This Act establishes a scheme to allow identification of vehicles, drivers and road users'. S150 (1)(d) provides that, 'A regulation may prescribe rules about the management of drivers, including for example requiring the keeping of a register of licences.'
[51] Queensland Transport, *New Queensland Driver Licence: Privacy Management Strategy* (2003) 3.

terms of the National Privacy Principles under the *Privacy Act*. This analysis raises issues similar to the collection, use and disclosure of personal and sensitive information already discussed. However, the statutory protections under the *Privacy Act* would most likely offer greater privacy protections, and clearer avenues of redress than is currently available to a NQDL-licence holder under *Information Standard No.42*, a mere administrative standard. However, there are also other, more fundamental issues associated with contracting out of government services in which there is a ''privatising' of the relationship between the service providers and members of the public, which has the potential to result in a loss for individuals of the benefits of administrative law'[52](for example, rights under the *Freedom of Information Act 1992* (Qld), and accountabilities of government under the *Financial Administration and Audit Act 1977* (Qld)). Potentially there is also the loss of ministerial responsibility and Parliamentary scrutiny.[53]

XI QUEENSLAND TRANSPORT LICENSING STAFF

The *NQDL Privacy Management Strategy*[54] provides that access to a licence-holder's personal information may be granted to authorised people including Queensland Transport licensing staff who will have access to licensing information on the microchip and the TRAILS database. The *Transport Operations (Road Use Management) Act 1995* already provides legislative authority for access to a driver licence-holder's personal information. For example, section 49(1) provides that 'an authorised officer may require a person to produce for inspection a document issued, or required to be kept, under a transport Act'; this includes officers and employees of the public service who have been appointed by the chief executive.[55] The breadth of this group of people includes transport compliance officers, administration officers,

[52] Gregorczuk H, '*Freedom of Information: Government Owned Corporations, Contractors and Cabinet Exemptions*' Research Bulletin No5/99, Queensland Parliamentary Library (1999), citing Hon Justice EW Thomas, 'Secrecy and Open Government', in PD Finn (ed), *Essays on Law and Government*,: *Principles and Values*, Vol 1 (1995) 182-227, 184.
[53] Administrative Review Council, Report to the Attorney-General, *The Contracting Out of Government Services*, Australian Commonwealth Government, (1998) vii.
[54] Queensland Transport, *New Queensland Driver Licence: Privacy Management Strategy*, (2003) 8.
[55] *Transport Operations (Road Use Management) Act 1995* (Qld) s 20, provides for the appointment of authorised officers, which includes 'every police officer'. Schedule 4 of the Act defines 'authorised officer' to mean 'a person who holds an appointment as an authorised officer under s 20.'

and police officers. The exceptions allowing disclosure in IPP 11 may serve to authorise the disclosure either because the individual would have been reasonably likely to have been aware of that kind of disclosure; or because it was authorised by law. However, if these exceptions are not sufficient to authorise the disclosure, then it may be that the 'consent' of the individual is required.

The *Privacy Act* defines 'consent' to mean 'express consent or implied consent'.[56] The ALRC *Discussion Paper* stated that its view on 'consent' is that, taking into account of 'how consent has been interpreted in Australia and overseas… there are four critical factors that apply…'[57] they are: the context in which the consent is sought; whether there is informed consent; whether the consent is voluntary; and whether the individual's option to consent to one purpose is freely available and not bundled with other purposes.[58]IS42 does not define 'consent', nor does it make any statement as to whether the definition of 'consent' from the *Privacy Act* is to be used. However, in the *IS42 Information Privacy Guidelines*[59] there is an explanatory discussion on 'consent' that provides '[t]he agency can safely use or disclose personal information under these exceptions <u>if the person the information is about clearly understands the use or disclosure they are consenting to, and they are not forced to consent.</u>' (My underlining).

The NQDL consultation materials do not provide sufficient information or detail in order for an individual or prospective NQDL-holder to provide 'informed consent' or 'voluntary consent'. To satisfy IPP 11, full details on the intended disclosure of information to any other person, including licensing staff and legislatively authorised officers must be documented and made available for consideration, for example, as part of the licence application forms.

---

[56] *Privacy Act 1988* (Cth) s6.
[57] Australian Law Reform Commission, *Review of Australian Privacy Law*, Discussion Paper 72 (2007) 578-579.
[58] Australian Law Reform Commission, *Review of Australian Privacy Law*, Discussion Paper 72 (2007) 578-579.
[59] *Information Standard 42: Information Privacy Guidelines*, V1.00.00 Queensland Government Information Architecture, 40 <http://209.85.173.104/search?q=cache:fuJGz0mHntwJ:www.qgcio.qld.gov.au/02_infostand/downloads/is42guidelines.pdf+information+standard+42&hl=en&ct=clnk&cd=5> at 10 September 2007.

One of the few means of legal redress for an unauthorised disclosure is provided for in section 143(1), *Transport Operations (Road Use Management) Act 1995*. This section provides that 'a person must not disclose, record or use information that the person gained through involvement in the administration of this Act, or because of an opportunity provided by the involvement.' This would apply to Queensland Transport staff accessing driver licensing information, binding them to confidentiality in their dealings with that information. The effectiveness of this provision may be reduced if an individual (whose information is disclosed) is not made aware of the disclosure.

XII INTERSTATE LICENSING AUTHORITIES

Queensland Transport currently has the power to release driver licence information and traffic offence histories without the consent of the licence holder. Section 77, *Transport Operations (Road Use Management) Act 1995* provides for both the release of this information in circumstances requiring the written consent of the licence-holder, and also the power of the chief executive to release information, without consent, about a person's Queensland driver licence or traffic offence history to a person who issues driver licences under a corresponding law.

The exchange of information is provided by the *Transport Operations (Road Use Management – Vehicle Registration) Regulation 1999* the *(TO(RUM–VR) Regulation*). In addition the *(TO(RUM–VR) Regulation* allows 'eligible people' and 'involved people' to obtain limited amounts of information in the form of certificates, and also provides for the 'National Exchange of Vehicle and Driver Information System' (NEVDIS). This system is operated under an arrangement with Queensland and other states that allows exchange of information about vehicles and drivers from the participating states. It is unlikely that this 'exchange' would be a breach of IPP 11 (or IPP 10 – limits on use of personal information) because IS42, as an administrative standard would not take priority over legislation or contractual arrangement.

This section would clearly include releasing the information for example, to the Victorian Department of Transport. The section also authorises 'an entity that, under an agreement between the State and other governments, maintains a database

containing information about driver licences and traffic histories' as being able to have access. Neither the *NQDL: Consultation Paper* nor the *NQDL Privacy Management Strategy* deal with the power to release information under *TO(RUM–VR) Regulation.*

There are examples of government organisations using personal information from databases for 'inappropriate purposes', for example, the New South Wales Ombudsman's report has on a number of occasions cited New South Wales police officers accessing databases inappropriately despite a code of practice[60] and UK driver licensing authorities have admitted selling information about vehicle licence owners to private companies.[61]

XIII ACCESS BY THE NQDL-HOLDER

The NQDL Proposal[62] includes the optional feature of offering secure online transactions to the NQDL-holder through the use of digital certificates. This feature will enable NQDL-holders to have access to license information details with the ability to update certain information including change of address details, via the smartcard partition relating to this information. Access to personal information and requirements for accuracy is provided for by IPPs 5, 6, 7 and 8. IPP 5 requires a record-keeper to provide an individual with information about their records; IPP 6 provides the individual with access to their own records; IPPs 7 and 8 require that the record it to be accurate, related to the purpose, up to date, complete and not misleading. The inclusion of the optional feature would be consistent with the information privacy principles.

XIV USE & DISCLOSURE TO QUEENSLAND POLICE SERVICE

[60] Greenleaf Graham, 'Ombudsman – Police still lax on disclosure, NSW Ombudsman Annual Report' (1994) 1(9) *Privacy Law and Policy Reporter*, 134, 175
[61] Stand, *Entitlement cards and identity fraud: Identity Card Response*, <http://www.stand.org.uk/IdCardResponse.html> at 20 April 2006.
[62] Queensland Transport, *New Queensland Driver Licence Proposal: Consultation Paper* (2003) 18

Under the NQDL Proposal, Queensland Transport are proposing two options to allow 'access by law enforcement and other government agencies'[63]to the digital photographs stored on the TRAILS database. Option A would allow 'access to photographs by law enforcement personnel and interstate licensing authorities'[64] This option includes the following 'protection measures: encryption of the photographs upon transfer and for storage; no storage of identifying personal information with the photograph; no data matching; and no ability to browse photographs'. Option A also provides clear limits on the circumstances in which the licensing authorities and law enforcement could access the photographs that relate to the investigations of fraudulent driver licences, criminal investigations under the *Transport Operations (Road Use Management) Act 1995*, or a court order or warrant 'specifically requesting release of a named licence holder's photograph'.[65]

In contrast, Option B provides a general statement that 'licence holders would be advised prior to applying for a licence that law enforcement personnel would have access to their photographs in much the same way they currently have access to other driving licensing information'.[66] This option allows 'law enforcement personnel to access digital photographs for law enforcement purposes, subject to clear accountability processes. Some of these purposes might include locating missing persons, identifying deceased persons involved in major accidents and their next of kin, executing warrants and serving other legal processes.'[67] There are significant privacy implications regarding this option. The broad use of the digital photograph for purposes unrelated to its collection would inevitably lead to 'function creep', that is the use of the TRAILS database for purposes for which it was not originally contemplated. The ALRC in its *Discussion Paper* included similar comments with respect to the Commonwealth Health and Social Services Access Card[68] that required a digital photograph as part of registration. The ALRC *Discussion Paper* included

[63] Queensland Transport, *New Queensland Driver Licence: Privacy Management Strategy* (2003) 4.
[64] Ibid.
[65] Ibid.
[66] Ibid 5.
[67] Ibid.
[68] The *Human Services (Enhanced Service Delivery) Bill 2007* (Cth) was passed by the House of Representatives on 28 February, and then introduced into the Senate on the same day, was adjourned and later withdrawn that same day.

comments that 'photographs of cardholders collected at the time of registration could later be used to identify people on Closed Circuit Television footage.' [69]

It is arguable that both Option A and Option B would be in breach of IS42, with respect to Information Privacy Principle 1, and the existing 'function provision' of the *Transport Operations (Road Use Management) Act 1995* because the personal information (the digital photograph) has been collected for the purpose of maintaining a driver licence register; the information has not been collected for the purpose of general law enforcement provisions. However, it is possible for Queensland Transport to establish that the information is necessary for one of its statutorily authorised purposes; in which case the subsequent use and disclosure (by Queensland Police Service) must be in compliance with IPP's 10 and 11. Although the *Transport Operations (Road Use Management) Act 1995* (sections 77 and 143) authorise access to driver licensing information to police officers, this authorisation is statutorily limited to transport related investigations.

Option A includes some limits on access to personal information, whilst Option B is drafted broadly in terms of access for 'law enforcement provisions'. Under Option B, Queensland Transport could be in breach of the confidentiality provisions of *Transport Operations (Road Use Management) Act 1995* section 77 (dealing with release of information from TRAILS), and section 143 (statutory duty of confidentiality), as well as breaches under IS42, under IPP 9 (personal information to be used for relevant purposes); IPP 10 (limits on use); and IPP 11 (limits on disclosure) by allowing Queensland Police Service access to personal information.

Under the options, the rationale for the disclosure on the basis of identification at an accident scene appears superfluous given the ability for a prospective NQDL-holder to be able to choose to provide emergency contact details that would specifically cover the circumstances for which the identification of a person at a major accident scene may be required.

[69] Australian Law Reform Commission, *Review of Australian Privacy Law*, Discussion Paper 72 (2007), 803 quoting A Stafford, 'Access Card Could Link to Surveillance', *The Age* (Melbourne), 5 June 2006 9.

Both of the options raise privacy issues: Queensland Police Service currently have the ability to access licensing information with respect to licensing or transport related investigations; why is it necessary for a licence-holder to give broad consent? What right would a licence-holder have to refuse to give that consent and still be able to obtain a licence, and have a guarantee that their photograph would not be accessed? The prospective NQDL-holder will have provided their personal information in the form of a digital photograph for the express purpose of enabling Queensland Transport to maintain a driver licence register. There is an element of compulsion in providing this personal information if a person chooses to drive a vehicle in Queensland.

Option A provides some clear guidance as to the circumstances in which the photographs will be released, and both options provide 'protection measures',[70] including: informing licence holders of their privacy rights; secure logins and use of trigger alarms for unauthorised access; maintaining and auditing transaction logs of licence photographs; conducting privacy training for relevant staff; promoting the availability of a privacy complaints resolution process; and enforcing penalties for improper use and disclosure. The use of technological (encryption and logins) and administrative (training and provision of information) means of protecting privacy need to occur within a context of providing a clear legislative right to the protection of information privacy. Although the NQDL Proposal states that penalties for improper use and disclosure will occur, within the current information privacy regime, this may not be effective (see the later discussion).

The protection measures are certainly appropriate to satisfy security measures and IPP 4; however, such measures are not to be confused with ensuring protection of the remaining IPPs dealing with use and disclosure. It is possible to breach information privacy through its use and disclosure, even though the personal information was stored in accordance with the principle relevant to security.

XV ACCURACY OF THE DIGITAL PHOTOGRAPH ON THE TRAILS DATABASE

[70] Queensland Transport, *New Queensland Driver Licence Proposal: Consultation Paper* (2003) 8.

Both Information Privacy Principles 7 and 8 require that reasonable steps in the circumstances be taken to ensure that personal information collected must be relevant, up-to-date, complete and accurate. The requirement of 'accuracy' of the database will raise information privacy issues under the proposed NQDL. Queensland Transport may experience technical difficulties in complying with the information privacy principles. For Queensland Transport to ensure the accuracy (or integrity as it is referred to by the consultation documentation) of the digital photographs, it will need to ensure that the database does not contain duplicate photographs, which are false identity photographs. Computer programs are available to scan through the database and identify where possible duplicates exist, however, research[71] conducted on such a program indicates that as the database size increases, the performance of the technology decreases by a significant percentage. The result is that the program may either falsely detect duplicate photographs, or fail to detect where the same person has been placed two (or more times) on the database. In terms of the proposed NQDL, it may mean that the database may still allow false driver licences to be issued by Queensland Transport; or that a genuine driver licence is wrongly asserted to be a false driver licence.

The inability to ensure the integrity of the digital photographs on the database will raise additional information privacy concerns if the Queensland Police Service relies upon the database for general 'law enforcement' functions. The standard of the IPP requires only that 'reasonable steps be taken' rather than requiring absolute accuracy.

XVI ENFORCEMENT ISSUES

The *NQDL Privacy Management Strategy* [i]provides that sanctions and remedies are in place under the *Transport Operations (Road Use Management) Act 1995* (Qld). Indeed a statutory confidentiality provision exists under this Act; [72] however, there is no penalty provided under the *State Penalties Enforcement Regulation 2000* (Qld) regarding breach of this provision.

[71] Phillips Jonathon, Grother Patrick, Micheals Ross, Blackburn Duane, Tabassi Elham, Bone Mike, 'Face Recognition Vendor Test 2002, Overview and Summary' (2003) *National Institute of Standards and Technology*, 2-3.
[72] *Transport Operations (Road Use Management) Act 1995* (Qld) ss77 & 143.

There are major difficulties in enforcing the information privacy principles under IS42 primarily because IS42 is only an administrative standard that can be superseded by legislative provisions or contractual clauses to the contrary. A further impediment is the scattered and complex nature of the administrative avenues for redress offered by the *Public Sector Ethics Act 1994; Public Service Act 1996;* and the *Financial Administration and Audit Act 1977.*

Finally, the remedies for breach of an individual's personal information are inappropriate. These matters are discussed in terms of accountabilities for breach by members of the public sector, with the focus on the Queensland Police Service, and Queensland Transport.

XVII ACCOUNTABILITY OF THE PUBLIC SECTOR

The *NQDL: Privacy Management Strategy* states[73] that accountability for breach of information privacy by members of the Queensland Police Service is in the *Police Service Administration Act 1990,* in which the offence of 'improper disclosure of information' is created. The offence incurs a monetary penalty which may not be an appropriate remedy to a NQDL-holder whose personal information has been disclosed improperly. It would be far more appropriate to establish penalties that address the subsequent loss of personal information privacy to the NQDL-holder as well as operate to deter the action of improper disclosure.

The enforcement of IS42 is through the *Public Sector Ethics Act 1994; Public Service Act 1996;* and the *Financial Administration and Audit Act 1977*. The *Public Sector Ethics Act* establishes an Integrity Commissioner, [74] however, there is no section providing for the Commissioner's function or powers. It merely establishes the need to prepare codes of conduct for public officials, and provides[75]that any disciplinary action for an approved code of conduct is to be dealt with, if the official is a public service officer by the *Public Service Act.*

[73] Queensland Transport, *New Queensland Driver Licence: Privacy Management Strategy* (2003) 5.
[74]*Public Sector Ethics Act 1994* (Qld) Part 7, Division 7.
[75]*Public Sector Ethics Act 1994* (Qld) s 24(a).

The *Public Service Act* provides [76]grounds for discipline: 'The employing authority may discipline an officer if the authority is reasonably satisfied that the officer has contravened, without reasonable excuse, a provision of this Act or a code of conduct.' Section 88, the *Public Service Act* provides the disciplinary action that may be taken as including termination of the officer's employment; reduce the officer's classification level and change the officer's duties accordingly; transfer or redeploy the officer to other employment in the public service; forfeit or defer a remuneration increment or increase of the officer; reduce the level of the officer's remuneration; impose a penalty on the officer of not more than the total of two of the officer's periodic remuneration payments; direct that a penalty imposed on the officer be deducted from the officer's periodic remuneration payments; reprimand the officer.' The range of disciplinary action available does not address in any way the loss suffered by a person whose privacy information has been breached, nor does it provide for any suitable remedy.

Similarly, under the Queensland Transport accountability regime that includes the *Code of Conduct 2003*[77]; a *Privacy Plan*; and a *Privacy Management Plan* there is an absence of appropriate remedies available to the aggrieved NQDL-holder. The *Code of Conduct 2003*[78] provides for 'managing breaches of the code' including: application of Queensland Transport's *Human Resources Policy & Procedure for Performance Improvement*, and *Human Resource Policy and Procedure for Discipline*; an 'assessment is to be made to identify the seriousness of the breach and the actual or possible impacts'. The assessment does not include reporting the breach to the licence holder. The penalties for a proven breach of this code range from reprimand through to dismissal, depending on the severity or seriousness of the breach and all the circumstances. There is no avenue for external review. Finally, although an 'Integrity Commissioner' is established under the *Public Sector Ethics Act 1994*, that statutory body has no power to review decisions made under the privacy plans or codes of conduct established under that Act.

[76] *Public Service Act 1996* (Qld) s87(1)(f).
[77] Queensland Transport, *Code of Conduct* (2005).
[78] Ibid 3.

None of the legislation, codes or plans offers any assistance with determining the follow matters: How does the NQDL-holder know that their information privacy has been breached; how will they prove the breach; and who will bear the expense of the litigation; who makes decisions on whether a breach has occurred; is the decision open to review and/or appeal; who has the burden of proving or disproving the breach. A member of the public seeking to determine the law that applies with respect to information privacy is provided with a combination of legislation; administrative standards; codes of conduct; and privacy plans. In short, a prospective NQDL-holder has no discernible legal rights relating to their information privacy, its management, review processes and enforcement.

XVIII INDEPENDENT PRIVACY MANAGEMENT COMMITTEE

Under the NQDL Proposal, it is proposed[79] to establish privacy oversight through the establishment of an 'independent privacy management committee' comprised of an 'independent chair and a balanced membership (for example, Queensland Transport, commercial partner, licence holders and privacy advocate)'.[80] The ability of the proposed committee to impartially protect privacy information interests is compromised due to its very composition of including Queensland Transport and the commercial partner who are 'interested parties' in the NQDL Proposal. Complaints made to this committee are again limited by the administrative nature of its establishment which means that it will be unable to provide an impartial, external approach to the aggrieved NQDL-holder.

The *NQDL Privacy Management Strategy*[81] has suggested a number of external avenues for complaint and appeal to the prospective NQDL-holder, including the Queensland Ombudsman and the Federal Privacy Commissioner. There are a number of issues in Queensland Transport's reliance on either avenue.

[79] Queensland Transport *New Queensland Driver Licence: Privacy Management Strategy* (2003) 12.
[80] Ibid.
[81] Ibid.

The Ombudsman, whose powers and functions are established under the *Ombudsman Act 2001 (Qld),* is subject to limitations on what can be investigated[82]which includes certain actions of Queensland Police Service officers where disciplinary action has been pursued under police legislation; where an action has been pursued under mediation; and actions being pursued by the auditor-general. The limitations on the Ombudsman may involve the very actions taken by Queensland Transport, which may require independent investigation.

The Ombudsman's Office already handles[83] over 7000 complaints a year, of which 5% of the existing complaints are not finalised. Queensland Transport already ranks in the top five departments against which complaints are lodged. It would be anticipated that in the first year of the introduction of the NQDL, if the Ombudsman's Office was relied upon to deal with complaints of NQDL-holders, this office could be unable to deal with the additional complaints. The use of either the Ombudsman's Office or the Federal Privacy Commissioner's office is contrary to Recommendation 6, made by the Legal, Constitutional and Administrative Review Committee, *Privacy in Queensland*[84] , that the functions of a Queensland privacy commissioner should not be combined with any other office.

XIX BROADER ISSUES ASSOCIATED WITH THE NQDL PROPOSAL

There are three broader issues associated with the NQDL Proposal: The compulsory nature of government requiring information which may negate the ability of the prospective NQDL-holder to provide consent; function creep in which the NQDL may be used for purposes beyond maintaining a driver license register; and that the NQDL may become a quasi-identity card.

XX COMPULSORY NATURE OF GOVERNMENT REQUIRING INFORMATION

[82] *Ombudsman Act 2001* (Qld) s16.
[83] Office of the Ombudsman, *Annual Report (2005 – 2006)* 37.
[84] Queensland Legal, Constitutional and Administrative Review Committee, *Privacy in Queensland,* Report no 9 (1998) 59.

The use of smartcard technology by government in its statutory requisition of information raises fundamental issues, including: does a citizen exercise any genuine choice in using this technology, in contrast to a 'consumer' for example electing to take up the use of a SIM-card in their mobile phone, or electing to use a loyalty scheme, who both chooses to participate in the technology, and consents to the collection and use of their information subject to specified limitations.

The proposed NQDL will include a number of points at which 'consent' will need to be expressly addressed to ensure prospective NQDL-holder's are considered fully informed of the use and disclosure of their personal information to which they are consenting. It is unlikely that Queensland Transport will offer a choice of participating in the NQDL; in fact this is the central issue of 'consent' with respect to a government organisation. If a person wishes to drive a vehicle in Queensland then they must obtain a driver licence, and after 2007, the only type of driver licence will be a smartcard driver licence; in this regard 'consent' is superfluous. However, there remain a number of other points at which the notion of 'consent' needs to be discussed, and obtained.

Consent, for it to be consent requires a consideration of whether the consent was informed and voluntary. The ALRC *Discussion Paper* commented on consent, considered account be taken of at least two 'critical factors': firstly, 'an analysis of the individual's likely level of understanding as to what he or she is consenting to, and the implications of giving and withholding his or her consent [and secondly] an analysis of whether the individual has a clear option not to consent…'[85] This analysis would best be addressed by Queensland Transport undertaking a full privacy impact assessment, and publishing the results. This would provide the prospective NQDL-holder with a level of knowledge that related directly and independently to each aspect of collecting personal information; using personal information; and disclosing personal information in order for consent to have been provided. The Queensland Transport consultation material does not refer to a privacy impact assessment having

[85] Australian Law Reform Commission, *Review of Australian Privacy Law*, Discussion Paper 72 (2007) 579.

been undertaken; however the Galexia website[86] states that they have conducted 'a Privacy Impact Assessment (PIA) of new technology being considered by Queensland Transport, including ongoing advice to the Department on smart cards, electronic authentication, digital certificates, evidence of identity, and PKI. Galexia's PIA and the subsequent *Privacy Management Strategy* received formal sign off from the Queensland Crown Solicitor and approval from a Cabinet sub-committee.'[87] To date, the privacy impact assessment has not been published.

XXI FUNCTION CREEP

Function creep has been defined as '…the tendency of systems to evolve such that they are used for purposes for which they were not designed, that never could have been envisaged at the time of system creation. … Security features, such as subject-privacy guarantees, are immensely difficult, if not impossible, to retrofit.' [88]

Queensland Transport have stated that other commercial applications be included on the smartcard as a means to offset smartcard technology costs. The NQDL Proposal in effect envisages a secondary use of the smartcard by other government agencies, for example, by allowing Queensland Police Service to access the database of digital photographs, and the inclusion of emergency contact details that may be accessed by emergency service officers. The beginning of 'function creep' is present in both instances of access to driver licence information by agencies not directly related to the function of maintaining a register of driver licence information.

Other States proposals for the use of smartcard driver licences, are being progressed with the intention to 'build in other applications', including that of the Victorian Government's *A Smarter Licence for Victorians* have stated in their proposal:[89] '…the overall aims of this study have been to adopt a simple solution initially but build in

[86] Galexia are specialist consultants in privacy who have been involved in providing advice on aspects of the NQDL project.
[87] Refer to Galexia's website <http://www.galexia.com/public/projects/projects-QT.html#Heading78> , at 10 January 2008.
[88] Stand, *Entitlement cards and identity fraud: Identity Card Response*, <http://www.stand.org.uk/IdCardResponse.html> at 20 April 2006 19.
[89] VicRoads, *Introducing New Driver Licence Card Technologies: A Smarter Licence for Victorians* (2002) 22.

capacity to expand to multiple applications as users become ready to accept new uses…' **(**My emphasis) The approach of Queensland Transport, and of VicRoads[90] to 'add on' applications is in contrast to the guidelines on how the privacy principles should be incorporated into smartcard projects, laid down by the Federal Privacy Commissioner.[91] The guidelines required that 'The purposes for which the card can be used must be settled at the beginning of the project's development; all parties to the smartcard project should be identified at the beginning of the project; card holders must be advised before there are any changes to the smartcard system (such as the introduction of new features) that affect the collection and use of personal information; their consent – real, informed consent – must be obtained to participate in the new arrangements. [92]

The only means to protect against (or at least reduce opportunities for) 'function creep' is to legislate for the information privacy principles, particularly the principles with respect to collection, use and disclosure.

XXII QUASI-IDENTITY CARD

Another issue associated with the NQDL Proposal is that it will become a 'quasi-identity card'. This is perhaps already an issue with a driver licence that is used as a means of identity by the commercial sector where it is regularly used to verify identity details in transactions such as accepting cheques. Although Queensland Transport does not promote the current driver licence as a means of identification, and its use in commercial transactions occurs independently, it will become more of an issue if Queensland Transport 'strengthens' its reliance as being an accurate means of identity for the driver licence purposes. It is likely that reliance on its use by the private sector will also increase.

XXIII CONCLUSION

[90] Ibid.
[91] Federal Privacy Commissioner, *Smart cards: Implications for privacy*, Information Paper No 4 (1995) 3.
[92] Ibid. The Canadian approach is to treat consent to each of these aspects – 'collection', 'use' and disclosure' as distinct and separate.

Technologies, including smartcards, are rapidly being developed with enormous capabilities to collect, use and disclose information about individuals. Government is increasingly the user and purchaser of this technology as a means of gaining the efficiency related benefits for carrying out its functions. As part of the balance in taking up these technologies, government must put in place legislative safeguards to protect individuals from possible costs to privacy incurred through the use of the technologies.

The conclusion then of this article is not that the NQDL Proposal should not be pursued as a means of fulfilling Queensland Transport's function to provide for registration and licensing of road users. Rather, that the NQDL Proposal should be implemented within a framework of dedicated privacy legislation (that is, a *Privacy Act (Qld*)) that protects an individual's information (both personal and sensitive) as a statutory right, rather than a principle that may be overridden by a contractual clause or by other legislation. A *Privacy Act (Qld)* is needed to provide the following: a statutory right to information privacy that at a minimum covers the IPPs; a clear right of legal redress for breaches of information privacy; appropriate remedies that address breaches; the requirement that a privacy impact assessment is to be carried out and published; the establishment of a privacy commissioner with the necessary functions, powers and resources to oversight privacy. In short, the earlier recommendations made almost ten years ago by the Queensland Legal, Constitutional and Administrative Review Committee in its review of privacy, need to be implemented.

[i] Queensland Transport, *New Queensland Driver Licence: Privacy Management Strategy* (2003) 13.